



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,783	12/04/2001	Timothy E. Moses	10500.01.7101	8446
23418	7590	09/23/2004	EXAMINER	
VEDDER PRICE KAUFMAN & KAMMHOLZ 222 N. LASALLE STREET CHICAGO, IL 60601				NGUYEN, MINH DIEU T
		ART UNIT		PAPER NUMBER
				2137

DATE MAILED: 09/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/004,783	MOSES ET AL.
	Examiner	Art Unit
	Minh Dieu Nguyen	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 27 May 2004.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 8,11-15,24 and 27-30 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 8,11-15,24 and 27-30 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date
4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. ____ .
5) Notice of Informal Patent Application (PTO-152)
6) Other:

DETAILED ACTION

1. Applicant's amendment and response dated May 27, 2004 have been entered with the amendments of claims 8 and 24 and the cancellation of claims 1-7, 9-10, 16-23, 25-26.

Claims 8, 11-15, 24, 27-30 are pending.

Response to Arguments

2. Applicant's arguments filed May 27, 2004 have been fully considered but they are not persuasive.

Perlman was not cited to show, nor was the reference alleged to show, that a user or group of end users can generate certificate update subscription information that include at least the identity of a plurality of subscriber subjects. It is the combination of Perlman (5,261,002) in view of Risch (5,471,629) that contains this feature. In the combination, providing the identity of at least one subscriber subject is inherent. This stems from the fact that Risch discloses sending a request to monitor an attribute. Identifying the attribute is necessary. When brought into the environment of Perlman, the monitored attribute is a subscriber and identifying that subscriber is necessary in the combination of those references. The feature of identifying that subscriber's public key is considered obvious as the monitored attribute is the subscriber's certificate, and the certificate contains the public key as per Perlman (col. 4, lines 5-10).

Applicant next traverses on the basis that Perlman reference does not teach using a blacklist by a server in order to allow a user to update its blacklist. Examiner respectfully disagrees, as this feature is taught by the Perlman reference. “The certification authority issues a signed blacklist periodically or on demand” (col. 3, lines 24-26) and “determining whether a user’s certificate is valid by first obtaining a copy of the certificate and a copy of the signed blacklist” (col. 4, lines 14-16). Thus, because the blacklist is issued periodically and a user gets a copy of signed blacklist when a certificate must be checked, the user effectively updates its blacklist.

On the topic of “there is no motivation to combine these references” as applicant states, examiner continues to maintain that the person of ordinary skill must possess both skills in database and public key certificates arts. This is not an unreasonable assumption since databases of certificates are being managed by the instant invention. Database is a broad field and certificates are a specific data that are being maintained in databases (both at the server and client). Combination of the references is further supported by the references themselves: Risch cites that monitored information may be employee information, while Perlman states that keeping employee certificates up-to-date is important in a public key infrastructure (PKI). The combination of references is implemented by the person of ordinary skill in the arts to which it pertains: database and PKI. Applicant may also note that the rejections of the independent claims cite that the *monitoring* feature of Risch is combined. As Risch is a secondary reference, not all features of Risch are present in combination of references. Risch teaches determining

which monitor attributes may have been affected, determining whether the values of any of the attributes have changed, and for each value which has changed notifying the client. This is exactly the feature combined with Perlman, and only this feature.

Claim Objections

3. Claim 27 is objected to because of the following informalities:

It includes "at least one of:" language which is followed by only one option.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims **8, 11-15, 24, 27-30** are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman et al. (5,261,002) in view of Risch (5,471,629).

a) **As to claims 8, 13-15, 24 and 29-30**, Perlman et al. discloses a method for updating a user's list of public key certificates issued by a certification authority on a

distributed communications system. In the invention, a public key certification authority issues a list of the certificates that have been revoked (called a "blacklist"), either periodically or on demand, in order to allow the user to update its list (col. 3, lines 24-28). This establishes the current state of the art with regards to public key certificates and that a user updating its list of public key certificates is well known in the art. Perlman does not provide a facility for monitoring a specific public key certificate in response to subscription information, nor notifying the user when it changes.

Risch discloses a method for monitoring changes in an attribute of an object on a database. This is analogous to the claim language of monitoring a certificate. As per col. 3, lines 58-68, monitoring begins after a client requests it, which corresponds to providing subscriber subject information. An example of an object on a database is given as information about an employee of a corporation (col.1, lines 28-60). The example given establishes that the invention of Risch is directly applicable to the monitoring of quantities (such as a public key certificate) associated with a specific user of a computer system. When an attribute changes, the client that requested the monitoring is notified of the change, which applies to the step of receiving an indication of a change while on-line. In col. 5, lines 45-60, Risch discloses the user updating its information based on the indication of change. The method of Risch is a procedure to be implemented by computer hardware, and therefore also comprises an apparatus. In col. 2, lines 45-56, Risch says a client may need to recomputed values that depend on the changed value. This is directly applicable to a public key, as it is used to compute ciphertext or to validate a signature.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the monitoring feature of Risch in the management of the public key certificates of Perlman so as to protect against attacks from a disgruntled employee, such as the one described in Perlman.

b) **As to claims 11 and 27**, the examiner takes official notice that it is well known to encrypt information related to security when transmitting it over a non-secure network.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the monitoring feature of Risch in the management of the public key certificates of Perlman so as to provide security against impersonating on networks.

c) **As to claims 12 and 28**, it would have been obvious and necessary step for one of ordinary skill in the art at the time of the invention to take in monitoring any attribute on a database. In order to monitor the attribute, its value must first be known, then compared with a previously known value. To determine the value, it must be accessed on the database, which constitutes pulling it from the database.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 703-305-9727. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 703-306-3036. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mon
mdn
9/16/04

Andrew Caldwell
Andrew Caldwell